Autor
Jürgen Kretschmer, Beauftragter für Informationssicherheit der SAKD

Veröffentlichungen

Sachsenlandkurier 06/22: Archive, Informationssicherheit, Dezember 2022

Homepage der SAKD:
https://www.sakd.de/ozg_informationssicherheit.html, Januar 2023

Entwicklungen in der Informationssicherheit bei der Umsetzung des Online-Zugangs-Gesetzes

Die SAKD ist vor reichlich einem Jahr im Sachsenlandkurier (Ausgabe 3/21 - September) unter dem Titel „Informationssicherheit bei der Umsetzung des Online-Zugangs- Gesetzes (OZG) durch sächsische Kommunen“ auf bestehende Normierungen und den damaligen Umsetzungsstand und dem sich daraus ergebenden Handlungsbedarf sowie auf die Bestandteile des Informationsverbundes einer Online-Anwendung und die Schutzziele der Informationssicherheit eingegangen[1].
Seitdem haben sich in diesem Umfeld zahlreiche Entwicklungen ergeben.

Das Bewusstsein für Informationssicherheit in den Kommunen hat sich, nicht zuletzt durch zentral bereit gestellte Informationen und Veranstaltungen, geschärft. Dies spiegelt sich auch in der zunehmenden Zahl an Benennungen von Beauftragten für Informationssicherheit wider.
Das Niveau der Informationssicherheit der Komponenten der kommunalen Referenzarchitektur wurde verbessert und auch auf Bundesebene werden die der Umsetzung des OZG zugrunde liegenden Prozesse durch weitere organisatorische und technische Vorgaben und Richtlinien greifbarer.
Neue Anforderungen ergeben sich aus der Kommunikation innerhalb des Portalverbundes von Bund und Ländern und der Nutzung von Einer-für-Alle-Diensten (EfA).

In diesem auf dem Artikel vom September 2021 aufbauenden Artikel sollen einzelne Entwicklungen näher betrachtet werden.

Voraussetzungen in den Kommunen

Folgte in den Kommunen die Informationssicherheit bisher oftmals selbst definierten Regeln, so ist die Verständigungsbasis in der OZG-Umsetzung und damit im Informationsverbund von Bund, Ländern und Kommunen zunehmend die BSI-IT-Grundschutzmethodik nach den Standards 200-x und dem zugehörigen Kompendium[2].

---

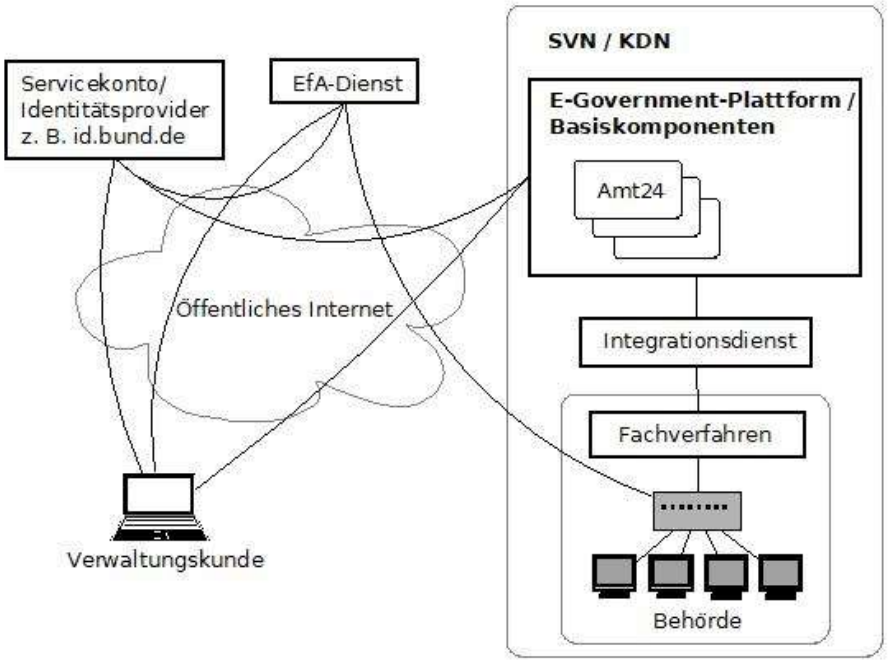
[1] SAKD: Artikel Informationssicherheit bei der Umsetzung des Online-Zugangs- Gesetzes (OZG) durch sächsische Kommunen September 2021
https://www.sakd.de/ozg_informationssicherheit.html
[2] BSI: IT-Grundschutz Informationssicherheit mit System
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Deren Anwendung wird im Sächsischen Informationssicherheitsgesetz[3] auch den nichtstaatlichen Stellen empfohlen. Die SAKD empfiehlt den Kommunen seit Ende 2021, die Standards als Basis aller Informationssicherheits-Aktivitäten zu verwenden und baut ihr Informations- und Schulungsangebot darauf auf.
Etwa die Hälfte der Kommunen ist dabei schon den ersten Schritt gegangen, einen Beauftragten für Informationssicherheit zu benennen. Sie bestimmen damit die Zuständigkeit im eigenen Hause und ermöglichen eine geregelte Kommunikation mit den koordinierenden und unterstützenden Stellen, wie dem Freistaat Sachsen, den sächsischen kommunalen Spitzenverbänden und der SAKD.
Mit weiteren Schulungen zum „BSI-IT-Grundschutz-Praktiker“ wurden im Oktober/November 2022 weitere kommunale Angestellte mit den Standards vertraut gemacht.
Eine Internetseite beim Freistaat[4] bündelt Angebote und verweist auf weitere Dienste und Informationen z. B. des SAX.CERT und der SAKD[5].
Diese Angebote werden fortgeführt und sollen die Kommunen dabei unterstützen, auch mit knappen Ressourcen der Informationssicherheit einen der Digitalisierung und Bedrohungslage angemessenen Stellenwert zu geben.

Der zu betrachtende Informationsverbund

Bestand letztes Jahr der betrachtete Informationsverbund aus den Komponenten des Verwaltungskunden, der sächsischen kommunalen Referenzarchitektur und der Kommunen, werden jetzt einige zusätzliche Bausteine für die Nutzung von Einer-für-Alle-Diensten (EfA)[6] und Funktionen des Portalverbundes einbezogen.

[3] Revosax: Sächsisches Informationssicherheitsgesetz
https://www.revosax.sachsen.de/vorschrift/18349-Saechsisches-Informationssicherheitsgesetz#p4
[4] Sächsische Staatskanzlei: Informationssicherheit in den Kommunen
https://www.egovernment.sachsen.de/informationssicherheit-in-den-kommunen-5657.html
[5] SAKD: ISMS nach BSI-IT-Grundschutzmethodik
https://www.sakd.de/is_isms_bsi_grundschutz.html
[6] BMI: Einer für Alle – Einfach erklärt
https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/nachnutzung/efa/efa.html



1 Typischer Informationsverbund schematisch

Mit dem bundesweiten EfA-Prinzip sollen bei der OZG-Umsetzung kostenintensive Mehrfachentwicklungen vermieden werden. Ein Anbieter entwickelt und betreibt einen Dienst und bietet diesen bundesweit allen Behörden zur Nutzung an. Damit vergrößert sich der zu betrachtende Informationsverbund um die Komponenten des EfA-Dienstes und die zwischenliegenden Netze.

Eine elementare Idee und Funktion des Portalverbundes ist es, das Verwaltungskunden mit nur einem Servicekonto bundesweit alle Verwaltungsdienste nutzen können und keine erneute Registrierung notwendig ist. Meldet sich ein Bürger z. B. an Amt24 mit der einem Nutzerkonto Bund zugehörigen Identität an, so lässt sich Amt24 die Authentisierung vom Bundesportal als Identitätsprovider bestätigen. Zur Anwendung kommt das Security Assertion Markup Language-Framework (SAML)[7].Die Verantwortlichkeit der Sicherheit dieser Funktion liegt bei Amt24.

Nichts geändert hat sich an der Gesamtverantwortlichkeit gegenüber dem Verwaltungskunden und an der Vorgehensweise. Die Kommune ist verantwortlich. Sie delegiert per Vertrag die Zuständigkeit außerhalb ihres Hoheitsgebietes an nachgelagerte Auftragnehmer und legt hierbei die BSI-IT-Grundschutz-Methodik zugrunde. Bedienen sich diese Aufragnehmer weiterer Subunternehmer, sollten sie der Kommune auch diese zusätzlichen Informationen konsistent und transparent zur Verfügung stellen.
Für die Nutzung der Basiskomponenten der sächsischen E-Government-Plattform haben die kommunalen Spitzenverbände stellvertretend mit dem Freistaat vor längerer Zeit eine Mitnutzungsvereinbarung[8] abgeschlossen.

---

[7]BSI: TR-03160-2 Interoperables Identitätsmanagement für Bürgerkonten (Seite 10: Ablauf einer SAML-Authentisierung)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03160/BSI-TR-03160-2.html

[8] Sächsische Staatskanzlei: Kommunale Mitnutzungsvereinbarung (nur aufrufbar aus KDN/SVN)
https://www.extranet.egovernment.sachsen.de/download/20191223_Kommunale_Mitnutzungsvereinbarung.pdf

Bietet die Kommune (EfA-) Dienste in eigener Hoheit an und/oder nutzt sie Identitätsprovider, ist sie dafür natürlich größtenteils selbst verantwortlich.

Für den Teil Amt24 des sächsischen Informationsverbundes hat der Beauftragte für Informationstechnologie (Chief Information Officer - CIO) des Freistaates im April 2022 in einem Schreiben an Bürgermeister und Landräte „das Serviceportal Amt24 für die Verarbeitung von Daten mit Schutzbedarf hoch freigegeben“. Die Verantwortlichen stellen die zugrunde liegenden Dokumente „den Basiskomponenten nutzenden Stellen bei Bedarf zur Einsicht zur Verfügung[9]“.
Eine Einsicht in die Informationssicherheitskonzepte ist in der Regel jedoch nicht zwingend erforderlich, da die konkreten Zuständigkeitsbereiche durch die Sächsische Staatskanzlei definiert wurden.

Für die Entwicklung und den Betrieb von Online-Antragsverfahren innerhalb des Amt24-Frameworks ist die Kommune weiterhin auch dann verantwortlich, wenn sie diese Dienstleistung durch Auftragnehmer, z. B. die Kommunale Informationsverarbeitung Sachsen (KISA)[10], erbringen lässt. Zur Darstellung der Abgrenzung der Verantwortlichkeit zwischen Amt24-Framework (Sächsische Staatskanzlei (SK)) und Online-Antragsverfahren (Kommune) stellt die SK ein Dokument zur Verfügung.

Eine ähnliche Erklärung zur Informationssicherheit wie für Amt24 liegt für die durch die Lecos GmbH betriebene OZG-Infrastruktur und den Integrationsdienst Transconnect (TC) für die Schutzziele Vertraulichkeit und Integrität vor. Demnach sind die „BSI Empfehlungen für einen hohen Schutzbedarf im Lecos-Rechenzentrum“ umgesetzt. Erhöhte Anforderungen an die Verfügbarkeit sind „gesondert zu bewerten“.

Die Netz- und Dienste-Infrastruktur des Sächsischen Verwaltungsnetzes (SVN) resp. des Kommunalen Datennetzes (KDN) verfügt über ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz[11], wobei Details nicht öffentlich zugänglich sind.

Idealerweise sollten alle eingesetzten Online-Dienste ebenfalls über entsprechende Zertifizierungen verfügen oder diese perspektivisch anstreben. In jedem Fall sollte der jeweilige Anbieter aber vertraglich zusichern, dass er das IT-Grundschutz-Vorgehen umsetzt und sein System entsprechend absichert.

Sicherheit Portalverbund des Bundes und der Länder

Der Portalverbund[12] verknüpft die Verwaltungsportale des Bundes und der Länder. Diese wiederum binden die Portale der Kommunen ein. Ziel des Verbundes ist es, dass ein Verwaltungskunde mit einer Registrierung alle Dienste im Verbund finden und nutzen kann - unabhängig davon, in welchem Portal sein Servicekonto beheimatet ist.

---

[9] Sächsische Staatskanzlei: Informationssicherheit (nur aufrufbar aus KDN/SVN) https://www.extranet.egovernment.sachsen.de/informationssicherheit.html
[10] KISA: Liste der Online-Anträge https://shop.kisa.it/64-online-antragsassistenten
[11] BSI: Liste der ISO 27001-Zertifikate auf der Basis von IT-Grundschutz https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/ErteilteZertifikate/iso27001zertifikate_node.html
[12] Bundesministerium des Innern und für Heimat: Startseite Portalverbund https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/portalverbund/portalverbund-node.html

Dazu müssen die Portale auf automatisierte und standardisierte Weise intensiv Daten, z. B. zu Zuständigkeiten, Identitäten und Dokumenten, austauschen. Diese intensive Kommunikation kann zur Folge haben, dass sich schädliche Aktivitäten schnell und weit im Verbund ausbreiten.
Um dem entgegen zu wirken hat das Bundesministerium des Innern und für Heimat (BMI) den §5 des Online-Zugangs-Gesetzes mit der IT-Sicherheitsverordnung Portalverbund (ITSiV-PV)[13] konkretisiert.
Diese Verordnung verpflichtet alle am Verbund Beteiligten, bestimmte Sicherheitsvorkehrungen zu treffen. Beim Umfang der Maßnahmen unterscheidet sie danach, ob technische Komponenten „unmittelbar" oder „mittelbar" angebunden sind. Eine unmittelbare Anbindung hat höhere Auflagen für die angebundenen Komponenten zur Folge.

Bei der Abwägung spielt vor allem eine Rolle, welches Schadenspotential angebundene Systeme haben und wie diese im Portalverbund abgewehrt werden können. Die Sächsische Staatskanzlei stellt dafür eine Handreichung zur Verfügung[14].
Bei einer Anbindung über eine „automatisierte Schnittstelle" wird von einem höheren Potential ausgegangen, was die Einstufung als „unmittelbare Anbindung" zur Folge hat. Weiteres Kriterium ist, ob hier Daten geschrieben oder nicht öffentliche Daten ausgelesen werden können. Es ergeben sich Auflagen wie Penetrationstests, Webchecks, Einhaltung bestimmter technischer Richtlinien und eine Absicherung nach der Vorgehensweise „Standardabsicherung".

Für Kommunen, welche die Dienste der Komm24 GmbH / KISA in Anspruch nehmen ist in der Regel von einer mittelbaren Anbindung der eigenen Systeme auszugehen. Verpflichtend nach ITSiV-PV ist demnach „nur" ein ISMS nach dem BSI-IT-Grundschutz mit der Vorgehensweise „Basisabsicherung".

Elektronischer Identitätsnachweis

Bei jeder elektronischen Kommunikation möchten sich die Kommunikationspartner darauf verlassen, dass die Gegenseite diejenige ist, als welche sie sich ausgibt.
Im Kontext der elektronischen Antragsstellung über Serviceportale wird die Authentizität des Betreibers des Portals über ein Serverzertifikat nachgewiesen. Amt24 verwendet ein „Extended Validation"-Zertifikat, welches durch den Vertrauensdiensteanbieter erst nach einem aufwändigen Validierungsprozess ausgestellt wird.
Der Verwaltungskunde kann sich bei Amt24 auf unterschiedliche Arten ausweisen. Mit Nutzername und Passwort lässt sich etwa ein grundlegendes Vertrauensniveau („Basisregistrierung") erreichen, welches für einfache Antragsverfahren genügt.
Die eID-Funktion des Personalausweises bzw. des elektronischen Aufenthaltstitels (elektronischer Identitätsnachweis) ist mit dem höchsten Niveau „hoch" universell anwendbar.
Dazwischen rangiert für Unternehmen die Anmeldung mit „Mein Unternehmenskonto"

[13] BMJ: Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten
http://www.gesetze-im-internet.de/itsiv-pv/
[14] Sächsische Staatskanzlei: IT-Sicherheitsverordnung Portalverbund (nur aufrufbar aus KDN/SVN)
https://www.extranet.egovernment.sachsen.de/it-sicherheitsverordnung-portalverbund.html

auf Basis des ELSTER-Unternehmenskontos[15], welche im Amt24 ab 2023 angeboten werden soll.

Gerade im Bereich der eID-Funktion des Personalausweises bzw. des elektronischen Aufenthaltstitels haben sich in letzter Zeit einige Entwicklungen vollzogen, mit welchen der bisher recht zögerliche Einsatz dieses Ausweisverfahrens überwunden werden könnte.
Das bisherige ungünstige Verhältnis zwischen Aufwand und nur gelegentlicher Nutzung hat sich verschoben. Mit der Ausweis-App[16] auf dem NFC[17]-fähigen Smartphone entfällt die Anschaffung eines Ausweislesers.
Immer mehr Anbieter[18] auch außerhalb der öffentlichen Verwaltung, wie Banken, Versicherungen, Krankenkassen, Mobilfunkanbieter und Identitätsdienste, bieten das Anmeldeverfahren an (Stand 06.10.2022: 186).
Ergänzend ist die Aktivierung der Funktion im Bürgeramt seit einiger Zeit kostenlos, genauso wie das Zurücksetzen des Passwortes. Für letzteres muss man auch kein Amt mehr aufsuchen, sondern kann das online erledigen[19].

Fazit

Die Digitalisierung von Verwaltungsvorgängen folgt der Erwartungshaltung von Bürgern und Unternehmen an eine moderne Verwaltung und ist nicht aufzuhalten.

Die Herausforderung für die Informationssicherheit besteht darin, hier angemessen Schritt zu halten. Deshalb müssen die Zuständigen von Beginn an in jedes Projekt einbezogen und die erforderlichen Mittel eingeplant werden. Ein diesbezügliches Versäumnis gefährdet die Handlungsfähigkeit und damit das Ansehen der Verwaltung.

Die unter Umständen komplette technische Auslagerung von Verwaltungsvorgängen erfordert ein Umdenken in der Organisation. Vom eigenen IT-Betrieb weitgehend losgelöste Prozesse werden durch Verträge mit Dienstleistern geregelt.

Gesetze, Verordnungen und Richtlinien bestimmen den Rahmen, dienen auch selbst als Hilfestellung und sind oft an weitere Unterstützungsmaßnahmen gekoppelt. Sie können jedoch die Motivation der Kommune nicht ersetzen.

Motivation geht einher mit Verständnis. Dieses für teils neue Themen zu fördern, war Ziel dieses Artikels. Über Ihr Feedback freut sich der Autor (E-Mail: kretschmer@sakd.de).

---

[15] Bayerisches Staatsministerium für Digitales: Startseite Mein Unternehmenskonto https://mein-unternehmenskonto.de/
[16] Governikus GmbH & Co. KG - im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik: Startseite Ausweis-App https://www.ausweisapp.bund.de/home/
[17] Wikipedia: Nahfeldkommunikation (NFC) https://de.wikipedia.org/wiki/Near_Field_Communication
[18] Bundesministerium des Innern und Heimat: Liste der Anwendungen https://www.personalausweisportal.de/SiteGlobals/Forms/Webs/PA/suche/anwendungensuche-formular.html
[19] Bundesministerium des Innern und für Heimat: Startseite PIN zurück setzen https://www.pin-ruecksetzbrief-bestellen.de/